updating the high-level protocol checksum takes the form of incrementally updating the checksum based on the obtained information about the network addresses of the first and second computer devices before and after network address translations.

23. [original] A method for maintaining the unchanged form of address translations performed by network address translation devices on encapsulated actual data packets transmitted with certain address information between a first computer device and a second computer device through a packet-switched data transmission network, the method comprising the step of

- forcing at least one of the first computer device and the second computer device to transmit to the other computer device keepalive packets with address information identical to that of actual data packets at a high enough frequency so that network address translation devices constantly reuse the mappings used for network address translation even when a certain fraction of the packets communicated between the first computer device and the second computer device are lost in the network.

REMARKS

Claims 1-23 were rejected as anticipated by the Nessett patent, 6,055,236.

With regard to the anticipation rejection, the Examiner is respectfully request to withdraw this rejection for the reason that not all elements of the claims at bar, as amended herein, are found in the Nessett patent, 6,055,236. Specifically, the claims at bar recite encapsulating packets conforming to a first protocol (such as IPsec) into packets conforming to a second protocol (such as TCP or UDP) which is capable of traversing network address translations and protocol conversions. **The amendments made in this response raise the point of distinction over Nessett that the**

encapsulation of the first protocol packets into the second protocol packets (tunneling) is only done if it is detected that network address translations are occurring and not otherwise. Because anticipation requires that every element of claim be present in the anticipating reference united in the same way to achieve the same result, the amendments here cause the claims to distinguish over Nessett.

At the passage cited by the Examiner at Col. 22, line 63 to column 23, line 29, Nessett teaches only conventional IPsec processing and does not teach the encapsulation technique of the invention to overcome the problems caused by Network Address Translation. Briefly, the problem with NAT and IPsec is that once an IP packet is protected by IPsec, it cannot be modified anywhere along the route to the IPsec destination. NAT routers violate this restriction by modifying packets. A further incompatibility is that NAT routers need to read the port numbers in TCP or UDP headers, and these values are encrypted in IPsec packets. These incompatibility problems are recognized by Nessett at Col. 25, lines 54-63.

The following passage from Col. 25, Lines 54 of Nessett (hereafter citations to column and line numbers will take the format Cxx/Lyy) shows that Nessett knows that prior art NAT routers are incompatible with IPsec packets when they process them and thus Nessett recognizes the same problem addressed by the invention:

> As was discussed above, NAT routers known in the art need to modify IP 48 packets. However, once an IP 48 packet is protected by IPsec, it cannot be modified anywhere along its path to the IPsec destination. NAT routers known in the art typically violate IPsec by modifying packets. In addition, even if a NAT router did not need to modify the packets it forwards, it must be able to read the TCP 58 or UDP 60 port numbers. If ESP is used by a local endpoint, the port numbers will be encrypted, so the NAT router will not be able to complete its required mapping.
>
> Local network devices on a LAN that use NAT possess only local, non-unique IP 48 addresses. These do not comprise a security name space that is suitable for

> binding a public key to a unique identity (i.e., a unique global IP 48 address). Without this binding, it is typically not possible to provide the authentication necessary for establishment of SAs. Without authentication, neither endpoint can be certain of the identity of their counter part, and thus cannot establish a secure and trusted connection via a SA. However, DNAT described above, can be used with IPsec to overcome some of the problems with NAT devices known in the art.

Nessett teaches a different way than the invention to get around these NAT-IPsec incompatibility problems by avoiding NAT altogether. This is done by doing a protocol called Distributed Network Address Translation (DNAT) instead of Network Address Translation. DNAT will be explained below.

The Nessett approach is different than the invention because Nessett avoids NAT altogether by substituting into his system an edge router (at the edge of the stub network or local LAN) which does DNAT instead of NAT by implementing a protocol called PAP. That means every LAN coupled to the internet by a router that does NAT must buy a new router that does DNAT when IPsec secure communications with hosts on the internet are to be carried out. The major problem with this approach is that if a protocol conversion happens between the source and destination which the DNAT edge router has no control over, the IPsec packets will fail to get through because the protocol conversions also require access to fields in the headers which are unavailable because of encryption of the fields by IPsec processing.

THE DIFFERENCE BETWEEN NESSETT AND THE CLAIMED INVENTION

In contrast, what the invention does is, if NAT or protocol conversions are found to be occurring between a source and a destination, is the following: the IPsec packets being sent from the source to the destination are encapsulated in packets have a protocol which NAT is compatible with such as TCP or UDP. In other words, the invention does not seek to avoid NAT altogether, it just tunnels through it so that IPsec packets get through and the NAT routers or protocol conversion entities can still do their

work. This has the advantage that the invention allows existing LANs with NAT routers to carry out secure communications using IPsec protocols without the need to buy new, specially adapted router.

THE PROBLEM ADDRESSED BY NESSETT

Nessett is addressed to the problem created by NAT of bogging down the network peformance of a stub network coupled to the internet via a NAT router caused by the computational load on the NAT router. The computational load, and resulting bottleneck, being referred to is described in the following passage from Col. 8, line 30 et seq.

> In network address translation schemes known in the art, the router 26 translates an internal network address such as an internal network address used on the first computer network 12 to an external network address such as a network address for outgoing traffic to the second network 30 or the third network 32. The router 26 also translates an external network address to an internal network address for incoming traffic from the second network 30 or the third network 32. A Network Address Translation ("NAT") router assumes the entire computation burden for network address translation. For large subnets, the NAT router becomes a bottleneck.

THE SOLUTION PROPOSED BY NESSETT

Nessett avoids the NAT bottleneck by elimination of computation and conversion of the addresses of inbound packets to new locally unique addresses for inbound packets and vice versa for outbound packets. This is done by introduction of a DNAT protocol which creates a unique combination address for every device on a stub network behind a DNAT router. The unique combination address for every device on the stub network is comprised of the globally unique IP address of the router of the stub network coupled with a port number which is unique to each process or device running on the stub network. The DNAT router maintains a table that maps each combination of globally unique IP address and unique port number to a corresponding locally unique IP address on the stub network. The combination network address is shown in Figure 7

The table that maps locally unique port numbersto internal network addresses is shown in Figure 8.

The advantage of this approach is that it eliminates the computational load of NAT and substitutes a simple table lookup.

The DNAT protocol of Nessett is described in the following passage from Col. 8, line 53 et seq.

In one preferred embodiment of the present invention, Distributed Network Access Translation ("DNAT") is used. Network devices (14, 16, 18, 22 and 24) on the first computer network 12

request a set of locally unique ports from the router 26 for external communications with the external second network 30 or the third network 32. A locally unique port is unique inside of the first

computer network 12 and typically is not unique outside of first computer network 12. Locally unique ports may be used for mobile network devices, such as device 20 using Mobile Internet

Protocol, that are not permanently attached to the first computer network 12. A mobile network device may physically relocate to another location and attach to a foreign computer network (i.e.,

other than home computer network 12).

> The network devices (14, 16, 18, 20, 22, 24) replace default or ephemeral ports with the locally unique ports and use a combination network address including a locally unique port and a common external network address (e.g., an IP address) for communications with the external networks 30 and 32. A default port is typically statically assigned. An ephemeral port is typically dynamically assigned for a specified duration of time.

The way DNAT works is shown in Figures 9 and 10 and described starting at Col. 13, line 33. The essence of DNAT is the combination address comprised of a locally unique

port number coupled with a globally unique IP address. This is explained in the following passage from Col. 13, line 61 et seq.

> The combination network address 72 includes a common IP 48 address (e.g., common network address 28) identifying network devices on the first computer network 12 to a second external computer network (e.g., 30 or 32). However, the present invention is not limited to the networks, network devices, network addresses or protocols described and others may also be used.
>
> The locally unique ports are used for entities such as protocols and applications in layered protocol stack 42 on a network device and are locally unique on the first computer network 12. The locally unique ports will identify a network device on the first computer network 12. For example, TCP 58 typically has a default port or ephemeral port assigned to the TCP 58 stack (e.g., 1234). After allocation with Method 130, a network device uses a locally unique port to replace a default or ephemeral port in a protocol layer in the layered protocol stack 42. As is illustrated in FIG. 8, the network device 14 with an internal IP 48 address, 10.0.0.1, is assigned thirty-two locally unique ports in the range of 1026-1057. The network device 14 may assign locally unique port-1032 to TCP 58 to use as a default or ephemeral port. An original default port or ephemeral for TCP 58 was 1234. The combination network address 112 illustrated in FIG. 7 is then assigned to TCP 58 on the network device 14 for communications with an external network (e.g., 30 or 32). Other locally unique ports are assigned to other protocols and applications in the layered protocol stack 42 on a network device to replace other default ports.

The advantage of DNAT taught by Nessett is found in the following passage from Col. 16, line 55 to Col. 17, line12:

> Distributed network address translation using Method 130 (FIG. 9) and Method 132 (FIG. 10) removes the computation burden of NAT at the router 26 and allows multiple network devices to use a single or a small number of external network addresses known to an external network such as the Internet or an intranet. Instead of providing NAT, the router 26 routes data packets from a network device (14, 16, 18, 20, 22, 24) on the first computer network 12 to a second external computer network such as the second computer network 30 or the third computer network 32 using the combination network address. In addition, the router 26 is no longer required to support multiple application protocols from the layered protocol stack 42.
>
> The router 26 also routes data packets from the second external computer network back to a network device on the first computer network using the locally unique port in the combination network address. The router 26 is no longer required to replace an internal network address with an external network address for outbound traffic, and replace an external network address with an

internal network address for inbound traffic. Thus, DNAT of the present invention removes the computational burden of NAT from the router 26 and does not violate the Internet principal of providing end-to-end transmission of data packets between network devices without alternations.

NESSETT'S IPsec SOLUTION USING DNAT

Nessett does teach tunnelling and encapsulation of one IP packet in another but the tunnelling is local tunnelling from a LAN device to the edge router. This is illustrated in the following passage from Col. 15, line 15 et seq.

> At Step 142, the network device 14 sends a TCP 58 request to the server 39 (FIG. 1). For example, a TCP 58 request for server 39 at external IP 48 address, 192.200.20.3, on the second computer network 30. Table 2 illustrates an exemplary request data packet sent at Step 142.
>
> Table 2 omitted
>
> The source IP 48 address is common external network address 28 (e.g., 198.10.20.30) and the source port is a locally unique port-1032 obtained via the PAP 64 with Method 130 and available to a TCP 58 service. In one embodiment of the present invention, the locally unique port-1032 replaces default port 1234 for TCP 58 when network device 14 was booted. In another embodiment ofthe present invention, default port 1234 is replaced with a locally a unique port, such as locally unique port-1032, whenever a protocol layer in layered protocol stack makes the request. The locally unique port along with the common external address comprise combination network address 112.
>
> In one preferred embodiment of the present invention, the default TCP 58 port of 1234 has been replaced with a locally unique port-1032. The destination IP address is, 192.200.20.3, for the server 39 (FIG. 1) on the second external network 30 and the destination port is well known Internet port 80. When the request reaches a network interface card device driver 44 in the layered protocol stack 42, an outer IP 48 header is added to route the request to the router 26. For example, the outer IP 48 is a virtual tunnel header that is explained below. Network interface card device drivers maintain the local internal network address (e.g., 10.0.0.x) for a network device for internal communications. Table 3 illustrates an exemplary data packet with an outer IP 48 header added for router 26.
>
> Table 3 omitted
>
> A network interface card device driver 44 adds the outer IP 48 header including (e.g., a virtual tunnel header) a source IP 48 address for network device 14 of, 10.0.0.1, and a destination IP 48 address of, 10.0.0.7, for the router 26. At Step 144, the router 26 receives the request data packet, strips the outer IP 48 header, and sends the request data packet to the external network 30.

So the original TCP/IP packet with the destination IP address of server out on the internet and the source IP address of the edge router in the IP header is originated in the TCP layer. The TCP layer includes in the combination address its locally unique port number 1032 as the source port in the TCP header. When that TCP/IP packet propagates down to the network interface card, the destination IP address and source port number are mapped into addresses in an outer IP header which will tunnel the IP packet to the edge router. What happens at the NIC is that the original TCP/IP packet is encapsulated into another IP packet with a source IP address 10.0.0.1 (locally unique only) of the LAN device whose TCP layer made the request and a destination IP address of the edge router 10.0.0.7 (locally unique only). This outer IP header is stripped off at the edge router and the inner TCP/IP packet is sent out on the internet.

To implement IPsec, the same procedure is used of encapsulating IPsec packets into other IP packets which tunnel the IPsec packets from the LAN device to the edge router where the outer IP packet header is stripped off. The IPsec packets are generally TCP/IP packets that have had AH and/or ESP headers added. The ESP headers encapsulate entire IP packets in tunnel mode or the upper layer protocol and the entire IP header in tunnel mode.

The edge router does DNAT as described above. It does not do NAT and there is no NAT address calculation and substitution in the IPsec packets as would be required by NAT. This is why the IPsec packets can be processed by the edge router in Nessett. There is no need in DNAT for the edge router to have access to the encrypted IP addresses in the inner IP packet.

The only difference between DNAT with IPsec and DNAT without IPsec is that the PAP protocol is used not only for LAN device to request locally unique ports from the

router but also to request locally unique SPIs from the edge router. This is shown from the following passages from Col. 26, line 8 et seq.

> A network device using DNAT as described above may also desire to establish a secure virtual connection to an external network device using IPsec (e.g., SPIs). Such a network device would request and use locally unique ports and use DNAT as was described above. In addition, the network device may request locally unique security values to use DNAT with IPsec.
>
> FIG. 19 is a flow diagram illustrating a Method 274 for distributed network address translation with security. At Step 276, a first network device on a first computer network requests with a first protocol, one or more locally unique security values (e.g., SPIs) from a second network device on the first computer network and for distributed network address translation. The one or more locally unique security values are used to identify security associations for data reception on the first network device during secure communications with a third network device on a second external network. At Step 278, the one or more locally unique security values are received on the first network device from the second network device with the first protocol. The one or more locally unique security values are stored on the first network device at Step 280. The one or more locally unique security values can be used to identify a unique security association for secure communications and used for distributed network address translation. A unique security association identified by the first computer on the first network is used for reception of packets on the first computer.
>
> In one exemplary preferred embodiment of the present invention, the first network device is a network device (14, 16, 18, 20, 22, and 24), the second network device is the router 26, the first protocol is the PAP 64, the one or more locally unique security values are SPIs used with IPsec, including AH or ESP. In one exemplary preferred embodiment of the present invention, the locally unique security values are obtained with the PAP 64 using a PAP 64 security request message 67, a PAP 64 security response message 69, and a PAP 64 security invalidate message 71.

So, unlike the invention, there is no tunnelling in Nessett of an IPsec packet encapsulated in a TCP or UDP packet through an edge router doing NAT and all the way through to the destination node or the tunnel endpoint. In Nessett, there is tunnelling of IPsec packets encapsulated in IP packets from the local LAN device only to the edge router and not beyond. This means that if the IPsec packet which emerges at the edge router after the outer IP packet is stripped later encounters any protocol conversion, the protocol

conversion will fail and the packet will not reach its destination.

THE CLAIMS AT BAR

The amended claims at bar are designed to provide a method to provide a way for packets conforming to a protocol such as IPsec which have not been able to traverse network address translation processes to be encapsulated in another packet type which can successfully traverse prior art network address translations when it is found that NAT is occurring. Specifically, in the preferred class of embodiments, IPsec packets are encapsulated into UDP or TCP packets which can be successfully transmitted across NAT, and then the IPsec packets are recovered at the destination.

WHY THERE IS NO ANTICIPATION

The amendments to the claims require the encapsulation of packets of the first protocol into packets of the second protocol only if it is discovered that NAT and/or protocol conversions happen between the transmitting device and the receiving device. Nessett does not teach this element. In Nessett, the tunnelling or P encapsulation between the LAN or stub network device and the router happens all the time and there is nothing conditional about it.

The terms NAT or network address translation and/or protocol conversions in the claims should be understood to mean the type of NAT or protocol conversions that require changing or access to information which cannot be changed or which is unavailable because it is encrypted in IPsec packets. This is another point of distinction over Nessett since the DNAT process does not require changing or access to anything in an IPsec packet which cannot be changed or to which access is unavailable.

This Nessett system is not the same method as described in the claims at bar when properly interpreted in accordance with the invention described in the specification

because the Nessett method cannot send IPsec packets across a NAT device as that term is properly interpreted. Properly interpreted, the claims of the invention generally call for determining what NATs and/or protocol conversions occur between the transmitter and receiver and, then, if NATs or protocol conversions are occurring, doing an encapsulation of the IPsec packets into packets of a protocol that can traverse as many NAT and protocol conversion devices as are encountered. **The NATs and protocol conversions being looked for are the prior art NAT and protocol conversions which require access to the IP addresses and port number in TCP headers which are not accessible in IPsec packets because of encryption.** The claims at bar, as properly interpreted, call for encapsulating packets of a protocol that cannot traverse NAT (such as IPsec -- same teaching applicable to protocol conversions also) in packets of a protocol that can traverse NAT (or protocol conversions) if NAT is occurring, transmitting these second protocol packets to the receiver and decapsulating them there to recover the packets of the original first protocol. No special routers or protocol converters are needed to practice the invention as is the case for Nessett.

In contrast, the Nessett method avoids the prior art NAT defined above and substitutes an edge router which does a protocol called DNAT which is not NAT as that term is used in the claims. DNAT requires a special edge router which understands the PAP protocol. If IPsec packets in Nessett's method encounter a true prior art NAT or protocol conversion device after they leave the edge router, they will be incompatible with it (because of encryption) and will not get to their destination.

With the invention, no special routers that do DNAT are needed and it does not matter how many NAT or protocol conversion devices are encountered. Futher, in the claimed invention, the transmitter and receiver do not need to understand or implement Nessett's PAP protocol or be able to send or receive PAP security messages.

Allowance is respectfully requested.

Respectfully submitted,

Dated: January 23, 2004

Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.
on January 23, 2004
(Date of Deposit)

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843